FortiClient (Windows) - Release Notes

Version 6.0.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
https://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

October 22, 2018
FortiClient (Windows) 6.0.3 Release Notes
04-603-513765-20181022

TABLE OF CONTENTS

Change Log **5**
Introduction **6**
Licensing 6
Standalone mode 6
Managed mode 6
Special Notices **8**
Microsoft Windows updates related to CPU security flaw (Meltdown) 8
Nested VPN tunnels 8
SSL VPN 98% issues 8
Windows notification of AV being disabled 8
Local certificate store not supported 8
Microsoft Windows server support 9
Rebranding tool not supported 9
What's New in FortiClient (Windows) 6.0.3 ..... **10**
Split DNS support for SSL VPN 10
Basic USB device control 10
Installation Information **11**
Firmware images and tools 11
Installation options 11
Upgrading from previous FortiClient versions 12
Downgrading to previous versions 12
Firmware image checksums 12
Product Integration and Support **13**
FortiClient 6.0.3 support 13
Language support 14
Conflicts with third party antivirus products 15
Resolved Issues **16**
Malware Protection 16
Web Filter 16
Application Firewall 16
Remote Access 17
GUI 18
Install and upgrade 18
Install and uninstall 18
Other 18
Known Issues **19**
Endpoint Control 19
Malware Protection 19
Web Filter 20
Application Firewall 20
Remote Access 20

GUI 21
Install and upgrade 21
Other 22

Change Log

Date	Change Description
2018-10-18	Initial release of FortiClient (Windows) 6.0.3.
2018-10-22	Added 483523 to Resolved Issues on page 16.

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.3 build 0155.

- Special Notices on page 8
- What's New in FortiClient (Windows) 6.0.3 on page 10
- Installation Information on page 11
- Product Integration and Support on page 13
- Resolved Issues on page 16
- Known Issues on page 19

Review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.

Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Managed mode

Companies with large installations of FortiClient usually need a means to manage their endpoints. EMS can be used to provision and centrally manage FortiClient endpoints, and FortiGate can be used with FortiClient endpoints for network security. Each FortiClient endpoint can connect to a FortiGate or an EMS. In this mode, FortiClient licensing is applied to the FortiGate or EMS. No separate license is required on FortiClient itself.

When using the ten (10) free licenses for FortiClient in managed mode, support is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided when using the free licenses. Phone support is provided for paid licenses.

FortiClient licenses on the FortiGate

FortiGate 30 series and higher models include a FortiClient license for ten (10) free, connected FortiClient endpoints. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

FortiClient licenses on the EMS

EMS includes a FortiClient license for ten (10) free, connected FortiClient endpoints for evaluation. For additional connected endpoints, you must purchase a FortiClient license subscription. Contact your Fortinet sales representative for information about FortiClient licenses.

Special Notices

Microsoft Windows updates related to CPU security flaw (Meltdown)

Microsoft Windows updates may not occur due to a CPU security flaw (Meltdown) with anti-virus products installed. Please read the customer service bulletin CSB-180105-1 at https://support.fortinet.com/Information/Bulletin.aspx. A PDF of the bulletin can be downloaded from the firmware download directory of the Fortinet support site at https://support.fortinet.com.

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN 98% issues

The new SSL VPN Windows driver, which was first introduced in FortiClient 5.6.0, resolves various SSL VPN connection issues. The new driver will help increase performance by up to 20% and provide a stable VPN connection.

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, the login timeout on the FortiGate can be increased to 180 seconds using the following CLI command:

```
configure vpl ssl settings
   set log-in timeout 180
```

Windows notification of AV being disabled

In FortiClient 6.0.3, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopped running.

Local certificate store not supported

FortiClient (Windows) no longer supports the local certificate store, and it is recommended you use Windows Certificates Store instead. If you are currently using the local certificate store, you should transition to Windows Certificates Store before upgrading to FortiClient (Windows) 6.0.3.

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Rebranding tool not supported

FortiClient (Windows) 6.0.3 does not support the FortiClient Rebranding Tool.

What's New in FortiClient (Windows) 6.0.3

This section identifies the new features and enhancements in FortiClient (Windows) 6.0.3. For more information, see the *FortiClient Administration Guide*.

Split DNS support for SSL VPN

FortiClient (Windows) now supports split DNS tunneling for SSL VPN.

Basic USB device control

You can use the USB device control feature to restrict access to USB ports on endpoints.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

File	Description
FortiClientSetup_6.0.xx.xxxx.exe	Standard installer for Microsoft Windows (32-bit)
FortiClientSetup_6.0.xx.xxxx.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientSetup_6.0.xx.xxxx_x64.exe	Standard installer for Microsoft Windows (64-bit)
FortiClientSetup_6.0.xx.xxxx_x64.zip	A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool
FortiClientTools_6.0.xx.xxxx.zip	A zip package containing miscellaneous tools, including VPN Automation files

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

File	Description
FortiClientVirusCleaner	A virus cleaner
OnlineInstaller	This file downloads and installs the latest FortiClient file from the public FDS
SSLVPNcmdline	Command line SSL VPN client
SupportUtils	Includes diagnostic, uninstallation, and reinstallation tools
VPNAutomation	A VPN automation tool

Please review the following sections prior to installing FortiClient version 6.0.3: Introduction on page 6, Special Notices on page 8, and Product Integration and Support on page 13.

Installation options

When installing FortiClient version 6.0.3, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You

can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall

It is recommended to not install VPN components on Windows Server systems if not required.

Upgrading from previous FortiClient versions

FortiClient version 6.0.3 supports upgrade from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Downgrading to previous versions

Downgrading FortiClient version 6.0.3 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 6.0.3 support

The following table lists version 6.0.3 product integration and support information.

FortiClient 6.0.3 support information

Desktop Operating Systems	• Microsoft Windows 7 (32-bit and 64-bit) • Microsoft Windows 8, 8.1 (32-bit and 64-bit) • Microsoft Windows 10 (32-bit and 64-bit) FortiClient 6.0.3 does not support Microsoft Windows XP and Microsoft Windows Vista.
Server Operating Systems	• Microsoft Windows Server 2008 R2 or newer FortiClient 6.0.3 does not support Windows Server Core.
Minimum System Requirements	• Microsoft Windows compatible computer with Intel processor or equivalent • Compatible operating system and minimum 512MB RAM • 600MB free hard disk space • Native Microsoft TCP/IP communication protocol • Native Microsoft PPP dialer for dial-up connections • Ethernet network interface controller (NIC) for network connections • Wireless adapter for wireless network connections • Adobe Acrobat Reader for viewing FortiClient documentation • Windows Installer MSI installer version 3.0 or later
FortiAnalyzer	• 6.0.0 and later • 5.6.0 and later
FortiAuthenticator	• 4.3.1 • 4.3.0 • 4.2.1 FortiToken Mobile push notification is not supported for the following versions: • 4.2.0 • 4.1.0 and later • 3.3.0 and later • 3.2.0 and later • 3.1.0 and later • 3.0.0 and later
FortiClient EMS	• 6.0.0 and later

FortiManager	• 6.0.0 and later • 5.6.0 and later
FortiOS	• 6.0.0 and later • 5.6.0 and later Only IPsec VPN and SSL VPN are supported with the following FortiOS versions: • 5.4.0 and later
FortiSandbox	• 3.0.0 and later • 2.5.0 and later The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command: `device-authorization -f` • 2.4.0 and later The following supported versions do not offer authorization of FortiClient: • 2.3.0 and later • 2.2.0 and later • 2.1.0

Language support

The following table lists FortiClient language support information.

Language	Graphical user interface	XML configuration	Documentation
English	Yes	Yes	Yes
Chinese (simplified)	Yes		
Chinese (traditional)	Yes		
French (France)	Yes		
German	Yes		
Japanese	Yes		
Korean	Yes		
Portuguese (Brazil)	Yes		
Russian	Yes		
Spanish (Spain)	Yes		

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

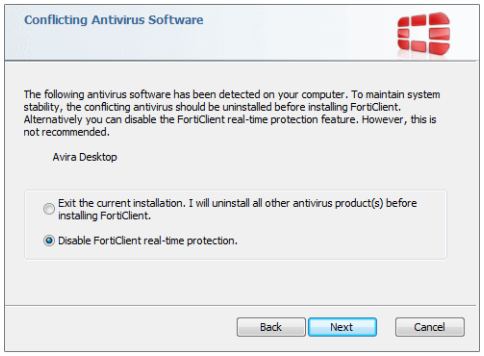
If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market.

- FortiClient's antivirus feature should not be used with other AV products.
- If not using FortiClient's antivirus feature, the FortiClient installation folder should be excluded from scanning for the third party AV product.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 6.0.3. For inquiries about a particular bug, contact Customer Service & Support.

Malware Protection

Bug ID	Description
477831	FortiClient (Windows) AV causes compilation error.
483523	Black screen for a few minutes after login/logoff.
507954	FortiClient (Windows) dashboard shows Sandbox as unauthorized even when the *Test* button shows it as valid.
511291	FortiClient (Windows) reports signature to be out-of-date if it is updated to the signature more than X days ago, regardless of version.
512236	AV RTP does not register to the Security Center in Windows 10 RS5.
512771	Skype-received files do not trigger Sandbox scan.
513591	Able to delete/restore quarantine file via virus alert popup when managed via EMS.
518062	FortiClient (Windows) failed to block USB access for the first insertion when using the system built-in policy to block USB access.

Web Filter

Bug ID	Description
469696	Safe Search does not work.
516012	FortiClient (Windows) Web Filter enable/disable setting change failed to apply.

Application Firewall

Bug ID	Description
509902	Application Firewall cannot be set to invisible.

Remote Access

Bug ID	Description
404746	SSL VPN with certificate authorization does not work from tray, but works from console.
450272	IPsec resiliency error message "'failed to launch IPsec service".
472223	Unable to select certificate for SSL VPN.
486712	Connecting to FortiGate clears authorized machine configuration (NAC node).
496190	Current personal VPN vibrates back to others in dual registration mode.
504185	FortiClient (Windows) console on Windows 7 PCs inaccessible in Windows system tray - SSL VPN failure.
508186	Phase 1/phase 2 IKE proposal not populated for IPv6 tunnel.
508392	With IPv6 as remote gateway, custom port changes to the default after editing/saving.
508400	Failed to remove split tunnel.
510060	*Save password*, *Auto-connect*, and *Always up* do not display when VPN is down.
510375	6.0.2 RC1 fails to connect to VPN from task tray with user certificate authentication (no username or password).
510748	If FortiClient (Windows) 5.6.x is installed on a different drive (E:\), manual upgrade to 6.0.x completes, but FortiClient (Windows) does not work after reboot.
510860	If *Prompt on connect* is selected, certificate filter does not work properly.
510945	Right-click is not working for username and password VPN fields.
511084	RSA new PIN mode does not work for IPsec v4/v6 tunnel.
511100	FortiClient (Windows) failed to switch auto-connect tunnels when FortiClient (Windows) is registered to FortiGate.
511110	FortiClient (Windows) VPN dashboard shows empty VPN tunnel after connecting from FortiTray.
511844	FortiClient (Windows) failed to show IP address for IPsec VPN.
513171	FortiClient (Windows) not displaying actual username used for SSL VPN tunnel.
513802	FortiClient (Windows) should report that VPN connection failed after two wrong passwords.
514666	Connected SSL VPN failed to display tunnel info when password contained special characters.
516090	FortiClient (Windows) IPsec VPN accepts invalid server certificate with IKEv2.
516156	Backing up and restoring FortiClient (Windows) causes loss of IPsec VPN pre-shared key.
516469	Should not display certificate dropdown for tunnel without certificate configured.

GUI

Bug ID	Description
492890	FortiClient (Windows) malware GUI says malware is quarantined when it is not.
511104	Default tab not working.
515821	Vulnerability schedule scan weekly is undefined in GUI.

Install and upgrade

Bug ID	Description
497115	GUI is blank.
505191	Remote Access (IPsec) loses saved username/password when upgrading to 6.0.0.
510335	Update Diagnostic Tool's collected information.
513716	Unable to upgrade FortiClient (Windows) 6.0.1 to 6.0.2 from EMS with password lock enabled.
517047	Fortitray.exe running PowerShell error prompt.
518212	Unable to open FortiClient (Windows) GUI in Windows 10 Education.

Install and uninstall

Bug ID	Description
510765	FortiClient (Windows) has many leftover files after uninstallation.

Other

Bug ID	Description
510979	Remembered FortiGate list needs to refresh after clicking *Forget*.
516401	MSFT_HW_API does not survive ephemeral Microsoft service outages.

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.3. For inquiries about a particular bug or to report a bug, contact Customer Service & Support.

Endpoint Control

Bug ID	Description
512783	FortiShield blocks FortiClient.exe from changing the registry.
516325	Software Inventory not showing all applications installed on the user PC.

Malware Protection

Bug ID	Description
481003	FortiClient causing longer logon time to terminal server(Citrix) for first user.
489052	Memory leak caused by FortiAptFilter.sys.
495880	Non-admin domain users can stop/pause USB media scans enforced by EMS configuration.
496084	AV exclusion list does not work in on-demand scan if %windir% or %systemroot% variables are used.
496326	FortiClient is sending intermittently files from local disk to the FortiSandbox for analysis.
499891	Scan on insertion does not work all the time.
507588	AV custom scan still scans files in the exclusion list.
509624	Newly installed FortiClient with RTP enabled does not disable Windows Defender's Real Time Protection on Windows 7.
514009	FortiClient (Windows) fails to inject into Firefox application.
516298	Windows 10 build 1803 reports *No Anti-Virus Installed* after FortiClient (Windows) 6.0.2 is installed via EMS.
516431	FortiClient (Windows) Sandbox still shows to submit trusted files on network driver.
516704	AV should recognize Windows signed files.
516841	FortiClient (Windows) Sandbox still holds files with sizes larger than 200 MB until timeout.
518018	FortiClient (Windows) failed to configure custom schedule AV scan for network path.

Bug ID	Description
518873	New empty line was added to the host file after each enable and then disable Safe Search configuration.
519096	FortiClient (Windows) failed to log USB block action for Google Pixel 2.
519098	Potential wrong block state for USB access after FortiClient (Windows) was uninstalled.
519213	FortiClient (Windows) failed to write on demand scan information to fclog.dat file.

Web Filter

Bug ID	Description
489821	FortiClient 5.6.6 and Windows 8.1 SSL error.

Application Firewall

Bug ID	Description
482920	FortiClient blocking DF set response.
509128	FortiClient 6.0.1 Application Firewall is blocking Avaya.

Remote Access

Bug ID	Description
450245	Need to add a switch for the number of auto-connect retries.
452476	FortiClient registers all interfaces' IP addresses to the DNS server, when SSL VPN tunnel is up.
486362	FortiClient 5.6.6 disables Windows IKE and AuthIP IPsec keying modules when connecting the VPN which effects MS direct access.
491407	FortiClient AutoConnect when Offnet not working (IPsec certificate).
502615	Without xAuth, connecting from FortiTray does not work properly.
504191	FortiClient connected via IPsec IKE (IPv4/v6 dual stack) unable to receive IPv6 address from the FortiGate.
504291	FortiClient with IPv6-only configuration fails to connect with remote IKE 2 IPv6 IPsec tunnel.
508650	Without xAuth, setting `<prompt_certificate>` to `0` with cert filter configured fails to make

Bug ID	Description
	VPN connection from FortiTray.
510735	6.0.2 RC1 fails to connect to VPN from task tray with user cert authentication - it prompts for certificate
515819	With cert filter configured, if *Save password* is enabled, should not prompt GUI during making VPN connection.
515937	ipsec.exe crashes in VCRUNTIME140.dll, version : 14.0.24210.0
516228	No error message for wrong IPsec VPN password when *Save password* and *Always up* are enabled.
516244	Changing/saving VPN setting should not remove IPv6 <remote_networks><network>.
516544	Cannot save username with certificate in SSL VPN (profile managed by EMS).
516717	*Empty username is not allowed* when using pushed tunnel without xAuth to connect from FortiTray.
516931	Standard user fails to establish VPN if choosing a tunnel that requires a certificate and connecting from FortiTray.
518061	Windows SSL VPN hostcheck by guid does not work.

GUI

Bug ID	Description
511436	Avatar setting was lost after logging out and logging in with a different user.
518103	Fails to connect to VPN from task tray with user certificate authentication (no username/password).

Install and upgrade

Bug ID	Description
497387	FortiClient Configurator should support automatic group assignment.
510748	If FortiClient (Windows) 5.6.x is installed on a different drive (E:\), manual upgrade to 6.0.x completes but FortiClient (Windows) does not work after reboot.
517242	FortiClient (Windows) failed to install FortiUmon.sys driver when upgrading from old FortiClient (Windows) with AV feature installed.

Bug ID	Description
518260	Unable to deploy-uninstall FortiClient (Windows) 6.0.3 build 0152 from EMS with password lock enabled.
518592	FortiClient (Windows) 6.0.3 failed to upgrade to new FortiClient version from FortiTray when using RDP session.

Other

Bug ID	Description
463956	Diagnostic Tool result does not have AV scan and RTP scan logs.
488842	Total uninstall 6.22.1 completely removing managed FortiClient.
502067	FortiClient (Windows) keeps prompting for reboot after connecting to EMS and finding a newer version.
506548	Vulnerability scan results do not display on EMS.
515473	Hiding any feature (except Application Firewall) causes FortiClient (Windows) to report feature as *Installed* and not *Enabled*.
515815	Unable to update from FDS.
516658	Disabling automatic maintenance from EMS does not delete the schedule in Windows client task scheduler.
517359	Observed FCDblog daemon crash on win81x86 platform.
518771	FortiShield blocks FortiClient.exe from changing the registry - FA_Scheduler.